

nkaliyamurthy 3/18/2024 ⇄

Computer Forensics Recap Discussion

A space for students to review and discuss key concepts from previous lectures.

What are the fundamental concepts of computer forensics, and why are they important in digital investigations

⇄ Preservation of evidence

Maintained authenticity of evidence

👍 0 🗨️ 0 📄 0

⇄ Helps provide concrete evidence in the court of law

👍 0 🗨️ 0 📄 0

⇄ Maintaining the integrity of the evidence

👍 0 🗨️ 0 📄 0

⇄ Analysing digital evidence

👍 0 🗨️ 0 📄 0

⇄ Keep evidences safe

👍 0 🗨️ 0 📄 0

⇄ Ensuring that the integrity of the data is intact

👍 0 🗨️ 0 📄 0

⇄ preserving and analysing forensic evidence

👍 0 🗨️ 0 📄 0

⇄ collect, examine, and safeguard evidence

👍 0 🗨️ 0 📄 0

⇄ **Fudemental conceots**

The fundemental concepts of computer forensics are data aquistion, recovery, analyssi and presentation.

👍 0 🗨️ 0 📄 0

⇄ **The fundamental concepts include understanding digital evidence, eDiscovery, and the role of**

processes and technologies in computer forensics. These concepts are crucial for properly handling, examining, and analyzing digital evidence to ensure its admissibility in legal proceedings.

👍 0 🗨️ 0 📄 0

What are the key steps in the computer forensics investigation process, and why is evidence handling crucial?

⇒ Chain of custody

👍 0 🗨️ 0 📄 0

⇒ The importance of the witness

👍 0 🗨️ 0 📄 0

⇒ Maintaining the scene and evidence

Securely capturing all evidence
Following procedures to maintain evidence, authority and custody to comply with the law
Complying with the law is crucial to support any criminal prosecution

👍 0 🗨️ 0 📄 0

⇒ **The key concept are preservation and identification**

👍 0 🗨️ 0 📄 0

⇒ preserving the evidence through chain of custody

👍 0 🗨️ 0 📄 0

⇒ Acquire the data: Gather, protect, and preserve the original evidence. Analyze the data: Examine and correlate digital evidence with events of interest.

👍 0 🗨️ 0 📄 0

⇒ **The investigation process involves evidence collection, handling, examination, analysis, and reporting. Proper evidence handling is critical to maintain the integrity of digital evidence, ensuring that it is not tampered with or compromised during the investigation.**

👍 0 🗨️ 0 📄 0

What are the characteristics of different types of disk drives, and how do they influence forensic analysis?

- ⇒ **SSD's have self cleaning partitions, making them harder to investigate**

👍 0 🗨️ 0 📄 0

- ⇒ Newer SSD's with Trim SD supporting OS's and garbage collection make deleted file or file carving much more difficult. Traditional magnetic drives are very well understood forensically but today's enormous capacities can be an issue in time and resources to search for evidence.

👍 0 🗨️ 0 📄 0

- ⇒ **Disk drives**

Hard drives are characterised by data read/write speeds. Mechanical hard drives are classified by how many times a second the internal disk rotates. Ssds are faster, quieter, smaller and more durable than hard disk drives they also consume less energy. They also offer easier data recovery if damaged useful for forensic investigation.

👍 0 🗨️ 0 📄 0

- ⇒ Overwritten and deleted data can be recovered but can be challenging.

👍 0 🗨️ 0 📄 0

- ⇒ **Disk drives vary in terms of technology (e.g., HDD, SSD) and storage capacity, which can impact data acquisition and analysis. Similarly, understanding file systems and using tools to examine them is essential for retrieving and interpreting digital evidence stored on disk drives.**

👍 0 🗨️ 0 📄 0

What are the fundamental principles of data acquisition in computer forensics, and why is methodology important?

- ⇒ **The process of imaging or collecting info from various media**

👍 0 🗨️ 0 📄 0

- ⇒ it must be verifiable and repeatable to ensure the admissibility of evidence in court

👍 0 🗨️ 0 📄 0

- ⇒ Acquiring the data in its rawest form as possible, making sure to not

introduce any changes, and verify that!!

👍 0 🗨️ 0 📄 0

- ⇒ **Data acquisition involves the systematic collection of digital evidence using forensically sound methods to preserve its integrity. Methodology ensures that evidence is collected in a manner that is admissible in court and withstands legal scrutiny.**

👍 0 🗨️ 0 📄 0

- ⇒ The gathering and recovery of sensitive data during a digital forensic investigation is known as data acquisition.

👍 0 🗨️ 0 📄 0

- ⇒ Methodology refers to the standardised and certified / validated tools and processes used to capture and analyse evidence.

👍 0 🗨️ 0 📄 0

What are anti-forensic techniques, and why do perpetrators employ them?

- ⇒ Destroying hardware containing files that may help in the forensics process.

They do this to prevent themselves being caught as just wiping the drive via software is usually not enough to cover your tracks

👍 0 🗨️ 0 📄 0

- ⇒ **Anti forensics**
They are techniques that makes the job harder and longer to do for forensic experts, they are used to cover better the data left by a crime.

👍 0 🗨️ 0 📄 0

- ⇒ Steps taken to hide or remove evidence to make the investigation harder for the forensic professionals.

👍 0 🗨️ 0 📄 0

- ⇒ Set of techniques used to sidetrack the forensic investigation process

👍 0 🗨️ 0 📄 0

- ⇒ Anti forensic techniques include encryption, hiding files in folders, obscuring file names to blend in. These techniques are used to delay forensic investigations

👍 0 🗨️ 0 🔄 0

- ⇒ For instance erased contents of a drive to make it harder then to analyse

👍 0 🗨️ 0 🔄 0

- ⇒ anti forensics are techniques employed to make data harder to find or recover

👍 0 🗨️ 0 🔄 0

- ⇒ Any techniques designed to obstruct or impair forensic evidence recovery. They are employed to prevent the collection or at least reduce the collection of digital evidence to their crimes and hinder any arrest or prosecution.

👍 0 🗨️ 0 🔄 0

- ⇒ Anti-forensic techniques are methods used by individuals to hinder digital forensic investigations. Some common anti-forensic techniques:

Data Encryption
File Deletion
Steganography
Data Fragmentation
File Timestamp Manipulation / Data Overwriting

Perpetrators employ these techniques to cover their tracks, evade detection, and prevent incriminating evidence from being discovered.

👍 0 🗨️ 0 🔄 0

- ⇒ **Anti-forensic techniques are methods used to hinder or manipulate digital investigations by obscuring or destroying evidence. Perpetrators use these techniques to evade detection and prosecution by law enforcement agencies.**

👍 0 🗨️ 0 🔄 0

